4. Propose a Mitigation Solution

After navigating the complexities of **web application incidents** your final task is to compile and present your findings in **a detailed incident report**

This report should not only document the attacks and vulnerabilities you encountered during the project tasks but also highlight any additional security weaknesses identified through your investigation.
The goal is to create **a comprehensive document** that could be presented to an organization to help them understand the incident and implement the proposed remediation strategies.

```
TIP: what is the thing that will limit the usage of the server
```

Report Guidelines:

Your report should be structured and detailed, adhering to professional standards. Consider using a Google Doc for its collaborative features and accessibility. Here are key elements to include:

1. **Introduction:** Briefly outline the attack, its impact, and the purpose of the report.
2. **Detailed Attack Analysis:** Analyze the attack, detailing the source, targeted endpoints, request volume, and tools used.
3. **Proposed Mitigation Strategy:** Present an effective mitigation plan to prevent future attacks.
4. **Justification for the Proposed Solution:** Explain why the proposed solution is the best option based on industry standards.
5. **Steps for Implementation:** Outline the necessary steps to implement the mitigation.
6. **Post-Implementation Monitoring:** Specify the tools and methods for ongoing monitoring post-implementation.
7. **Conclusion:** Summarize the report, emphasizing the importance of the solution and future security.